From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] Exploiting cyclotomics for fast norms in filtered-S-unit attacks
Date: Sunday, July 31, 2022 10:37:38 AM ET
Attachments: smime.p7m

I'm pleased to announce availability of the next installment in the S-unit-attacks saga: a new 59-page paper "Fast norm computation in smooth-degree Abelian number fields", to appear at the upcoming Algorithmic Number Theory Symposium.

This paper is backed by an "abelianfields" software package with thousands of lines of Sage scripts testing the paper's main algorithms, and a smaller "cyclo2power" C software package demonstrating concrete speeds achieved for the easier case of power-of-2 cyclotomic fields.

The computational bottleneck addressed here is computing norms of many small number-field elements. This is one of the central bottlenecks in filtered-S-unit attacks against Ideal-SVP. It is also one of the central bottlenecks in traditional class-group and unit-group computations, two of the main tasks of computational algebraic number theory. There are decades of earlier literature on algorithms handling this bottleneck for general number fields.

The new paper and software show how to handle this bottleneck much more efficiently for smooth-degree cyclotomic fields than any approach known for general number fields. Concretely, the speedup factor is above 100000 at sizes of cryptographic interest.

Major contributions to this speedup include automorphisms (trivially) and subfields (the main topic of the paper). Further details, including the paper and the software, are available here:

   https://s-unit.attacks.cr.yp.to/norms.html

One should not think that this speedup is appearing all at once out of nowhere; see the paper for credits to the relevant literature.

More broadly, there is already a long history in algebraic number theory of problems that have been intensively studied for general number fields and shown to have particularly efficient solutions for the extreme case of cyclotomic fields. For examples and references, see Section 2.6 of the following paper:

   https://ntruprime.cr.yp.to/latticerisks-20211031.pdf

For the relevance of cyclotomic weaknesses to the management of risks in post-quantum cryptography, see Sections 1.3, 2.3, and 2.5 of that paper.

———D. J. Bernstein